

AMENDED IN ASSEMBLY JULY 3, 2008
AMENDED IN ASSEMBLY JUNE 17, 2008
AMENDED IN ASSEMBLY JUNE 5, 2008
AMENDED IN SENATE JANUARY 7, 2008
AMENDED IN SENATE APRIL 17, 2007
AMENDED IN SENATE MARCH 20, 2007

SENATE BILL

No. 31

Introduced by Senator Simitian

December 4, 2006

An act to add Title 1.80 (commencing with Section 1798.79) to Part 4 of Division 3 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 31, as amended, Simitian. Identification documents.

The Information Practices Act of 1977 regulates the collection and disclosure of personal information regarding individuals by state agencies, except as specified. Existing law also prohibits certain business entities, as defined, from making specified disclosures in relation to individual consumer records.

This bill would provide that a person or entity that intentionally remotely reads or attempts to remotely read a person's identification document using radio-waves *frequency identification (RFID)* without his or her knowledge and prior consent, as described, shall be punished by imprisonment in a county jail for up to one year, a fine of not more than \$1,500, or both that fine and imprisonment, except as specified. The bill would also provide that a person or entity that knowingly

discloses, or causes to be disclosed, specified operational system keys shall be punished by imprisonment in a county jail for up to one year, a fine of not more than \$1,500, or both that fine and imprisonment.

~~By imprisonment.~~ By creating new crimes, this bill would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: yes.

The people of the State of California do enact as follows:

1 SECTION 1. The Legislature hereby finds and declares all of
2 the following:

3 (a) The right to privacy is a personal and fundamental right
4 protected by Section 1 of Article I of the California Constitution
5 and by the United States Constitution. All individuals have a right
6 of privacy in information pertaining to them.

7 (b) This state has previously recognized the importance of
8 protecting the confidentiality and privacy of an individual's
9 personal information contained in identification documents such
10 as driver's licenses.

11 SEC. 2. Title 1.80 (commencing with Section 1798.79) is added
12 to Part 4 of Division 3 of the Civil Code, to read:

13
14 TITLE 1.80. IDENTIFICATION DOCUMENTS
15

16 1798.79. (a) Except as provided in ~~subdivisions (c) and (d)~~
17 *this section*, a person or entity that intentionally remotely reads or
18 attempts to remotely read a person's identification document using
19 radio ~~waves~~ *frequency identification (RFID)*, for the purpose of
20 reading that person's identification document without that person's
21 knowledge and prior consent, shall be punished by imprisonment
22 in a county jail for up to one year, a fine of not more than one
23 thousand five hundred dollars (\$1,500), or both that fine and
24 imprisonment.

1 (b) A person or entity that knowingly discloses, or causes to be
2 disclosed, the operational system keys used in a contactless
3 identification document system shall be punished by imprisonment
4 in a county jail for up to one year, a fine of not more than one
5 thousand five hundred dollars (\$1,500), or both that fine and
6 imprisonment.

7 (c) Subdivision (a) shall not apply to:

8 (1) The reading of a person's identification document for triage
9 or medical care during a disaster and immediate hospitalization or
10 immediate outpatient care directly related to a disaster, as defined
11 by the local emergency medical services agency organized under
12 Section 1797.200 of the Health and Safety Code.

13 (2) The reading of a person's identification document by a health
14 care professional for reasons relating to the health or safety of that
15 person or an identification document issued to a patient by
16 emergency services.

17 (3) The reading of an identification document of a person who
18 is incarcerated in the state prison or a county jail, detained in a
19 juvenile facility operated by the Division of Juvenile Facilities in
20 the Department of Corrections and Rehabilitation, or housed in a
21 mental health facility, pursuant to a court order after having been
22 charged with a crime, or to a person pursuant to a court-ordered
23 electronic monitoring.

24 (4) Law enforcement or government personnel who need to
25 read a lost identification document when the owner is unavailable
26 for notice, knowledge, or consent, or those parties specifically
27 authorized by law enforcement or government personnel for the
28 limited purpose of reading a lost identification document when
29 the owner is unavailable for notice, knowledge, or consent.

30 (5) Law enforcement personnel who need to read a person's
31 identification document after an accident in which the person is
32 unavailable for notice, knowledge, or consent.

33 (6) Law enforcement personnel who need to read a person's
34 identification document pursuant to a search warrant.

35 ~~(7) The reading of a person's identification document in the~~
36 ~~course of an act of good faith security research, experimentation,~~
37 ~~or scientific inquiry, including, but not limited to, activities useful~~
38 ~~in identifying and analyzing security flaws and vulnerabilities.~~

39 ~~(8) A person or entity that in the course of operating its own~~
40 ~~contactless identification document system inadvertently reads or~~

1 collects data from another contactless identification document
2 system, if once the person or entity becomes aware that it has
3 inadvertently read or collected data, it does not do any of the
4 following:

5 (A) Disclose the data to another party.

6 (B) Use the data for any purpose without the consent of the
7 person to whom the data pertains.

8 (C) Store the data without the consent of the person to whom
9 the data pertains.

10 (d) Subdivision (a) shall not apply to a person or entity that
11 unintentionally remotely reads a person's identification document
12 using RFID in the course of operating a contactless identification
13 document system unless it knows it unintentionally read the
14 document and thereafter intentionally does any of the following
15 acts:

16 (1) Discloses what it read to a third party whose purpose is to
17 read a person's identification document, or any information
18 derived therefrom, without that person's knowledge and consent.

19 (2) Stores what it read for the purpose of reading a person's
20 identification document, or any information derived therefrom,
21 without that person's knowledge and prior consent.

22 (3) Uses what it read for the purpose of reading a person's
23 identification document, or any information derived therefrom,
24 without that person's knowledge and prior consent.

25 (e) Subdivisions (a) and (d) shall not apply to the reading,
26 storage, use, or disclosure to a third party of a person's
27 identification document, or information derived therefrom, in the
28 course of an act of good faith security research, experimentation,
29 or scientific inquiry, including, but not limited to, activities useful
30 in identifying and analyzing security flaws and vulnerabilities.

31 ~~(d)~~

32 (f) Nothing in this section shall affect the existing rights of law
33 enforcement to access data stored electronically on driver's
34 licenses.

35 ~~(e)~~

36 (g) The penalties set forth in subdivisions (a) and (b) are
37 independent of, and do not supersede, any other penalties provided
38 by state law, and in the case of any conflict, the greater penalties
39 shall apply.

1798.795. For purposes of this title, the following definitions shall apply:

(a) “Contactless identification document system” means a group of identification documents issued and operated under a single authority that use ~~radio waves~~ *RFID* to transmit data remotely to readers intended to read that data. In a contactless identification document system, every reader must be able to read every identification document in the system.

(b) “Data” means any information stored or transmitted on an identification document in machine-readable form.

(c) “Identification document” means any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity. Identification documents specifically include, but are not limited to, the following:

(1) Driver’s licenses or identification cards issued pursuant to Section 13000 of the Vehicle Code.

(2) Identification cards for employees or contractors.

(3) Identification cards issued by educational institutions.

(4) Health insurance or benefit cards.

(5) Benefit cards issued in conjunction with any government-supported aid program.

(6) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the Business and Professions Code.

(7) Library cards issued by any public library.

(d) “Key” means a string of bits of information used as part of a cryptographic algorithm used in encryption.

(e) “Radio frequency identification” or “RFID” means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

~~(e)~~

(f) “Reader” means a scanning device that is capable of using ~~radio waves~~ *RFID* to communicate with an identification document and read the data transmitted by that identification document.

~~(f)~~

1 (g) “Remotely” means that no physical contact between the
2 identification document and a reader is necessary in order to
3 transmit data using ~~radio waves~~ *RFID*.

4 SEC. 3. No reimbursement is required by this act pursuant to
5 Section 6 of Article XIII B of the California Constitution because
6 the only costs that may be incurred by a local agency or school
7 district will be incurred because this act creates a new crime or
8 infraction, eliminates a crime or infraction, or changes the penalty
9 for a crime or infraction, within the meaning of Section 17556 of
10 the Government Code, or changes the definition of a crime within
11 the meaning of Section 6 of Article XIII B of the California
12 Constitution.